Аннотация дипломной работы

Тема: Определение наличия вредоносного программного обеспечения по сетевому трафику

ФИО студента: Литвиненок Александра Павловна

Научный руководитель: Головач Александр Леонидович, ассистент кафедры технологий программирования; Курбацкий Александр Николаевич, профессор, доктор технических наук

Кафедра (специальность, специализация): Кафедра технологий программирования (компьютерная безопасность)

Объем: 46 с., 9 рис., 2 табл., 16 источников, 2 приложения

Ключевые слова: ВРЕДОНОСНОЕ ПО, НЕЖЕЛАТЕЛЬНОЕ ПО, СЕТЕВОЙ ТРАФИК, DNS, ТУННЕЛИРОВАНИЕ, ЗАХВАТ ТРАФИКА, АНАЛИЗ ТРАФИКА

Цель работы (постановка задачи): Целью данной дипломной работы является исследование сетевого трафика на присутствие в нем следов нежелательного программного обеспечения, возможность сокрытия в передаваемом трафике произвольных данных и разработка приложения, способного анализировать захваченный трафик и выявлять в нем наличие сокрытых данных.

Описание работы студента: в данной дипломной работе были исследованы варианты сокрытия передаваемых данных, дана классификация нежелательного ПО, рассмотрены методы перехвата и анализа трафика с целью поиска в нем следов деятельности вредоносного ПО, даны признаки, по которым в трафике может быть обнаружено вредоносное ПО, рассматривается реализация сокрытия передаваемых данных на основе туннелирования в протоколе DNS, приведено описание приложения, доказывающего возможность реализации темы работы.